(2)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-105545
(43)Date of publication of application : 10.05.1988

(51)Int.Cl. H04L 9/02

(21)Application number : 61-251247
(22)Date of filing : 22.10.1986

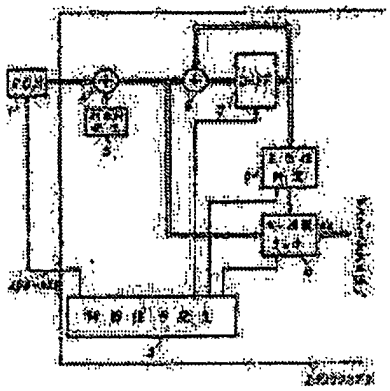
(71)Applicant : SONY CORP
(72)Inventor : EMOTO HARUICHI

(54) DECODER

(57)Abstract:

PURPOSE: To prevent a cryptographic algorithm from being decoded by not handling it as key information so long as the key information from a storage device is not correct in a decoder using the key information from the storage device so as to decode the cryptographic information signal.

CONSTITUTION: A check bit is written in a ROM 1 in addition to the key information and the information is read sequentially and repetitively as a parallel data by using sequential address signals ADϕ ~ AD3 from a control signal generator 3. Then M-series is decoded by an EX-OR circuit 4 and the result is fed to a D-FF7 and a latch circuit 10 via an EX-OR circuit 6. A data from the EX-OR circuit 6 is latched in the D-FF7 at the 1st ~ 4th periods when the data is read repetitively from the ROM 1. An adequacy discriminating circuit 9 discriminates all the data latched in the D-FF 7 to be a prescribed value at the end of the 1st ~ 4th periods, then the latch circuit 10 is operated. Then key information KI latched by the latch circuit 10 is fed to a descrambler main body, where decoding is processed.



In the above configuration, when the key information as the data from the ROM (1) is legitimate, the data latched by the D-FF (7) is set to a predetermined value. The latch circuit (10) is set in an operating state by the legitimacy determining circuit (9). The key information KI is latched by the latch circuit (10). The key information KI is supplied to the descrambler body to be decrypted. On the other hand, when the key information as the data from the ROM (1) is not legitimate, the data latched by the D-FF (7) is not set to the predetermined value. The latch circuit (10) is not set in an operating state by the legitimacy determining circuit (9). The key information is not latched by the latch circuit (10). Thus, the key information in this case is not supplied to the descrambler body, nor treated as key information.

Therefore, according to this example, for example, when the key information is tampered with to be illegitimate, the key information is not supplied to the descrambler body, nor treated as key information. This results in a difficulty of deciphering an encryption algorithm by tampering with the key information or the like. According to this example, the data are determined to be legitimate when the data latched by the D-FF (7) are all set to predetermined values at the end of the first to fourth cycles, providing an advantage of highly accurate determination.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63－105545

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)5月10日
H 04 L 9/02		Z－7240－5K	

審査請求　未請求　発明の数 1　(全4頁)

⑤発明の名称　復号化装置

㉑特　願　昭61－251247

㉒出　願　昭61(1986)10月22日

㉗発明者　江本　晴一　東京都品川区北品川6丁目7番35号　ソニー株式会社内

㉑出願人　ソニー株式会社　東京都品川区北品川6丁目7番35号

㉔代理人　弁理士 伊藤　貞　外1名

明　細　書

発明の名称　復号化装置

特許請求の範囲

記憶装置からのキー情報により暗号化された情報信号を復号するものにおいて、

上記記憶装置に上記キー情報領域の他にチェックビット領域が設けられ、復号時上記記憶装置のキー情報及びチェックビットが選択的に繰り返し指定されて論理演算がなされ、この演算結果が所定値となるときのみ、上記キー情報により暗号化された情報信号の復号化が行なわれることを特徴とする復号化装置。

発明の詳細な説明

(産業上の利用分野)

本発明は、例えばスクランブル通信システムのデスクランブラに適用して好適な復号化装置に関する。

(発明の概要)

本発明は、記憶装置からのキー情報により暗号化された情報信号を復号化する復号化装置において、記憶装置からのキー情報が正当なものではない限り、キー情報として取扱わないようにしたことにより、暗号化のアルゴリズムが解読されるのを防止するようにしたものである。

(従来の技術)

第3図はスクランブル通信システムの一例を示すものである。同図において、端子(21)には、ビデオ、オーディオ、データ等の情報信号S1が供給される。この情報信号S1はスクランブラ(22)に供給されて所定のアルゴリズムをもって暗号化される。このスクランブラ(22)より出力される暗号化された情報信号S1*は、送信機(23)に供給される。そして、この送信機(23)より、通信回線(24)、例えば通信衛星等を介して受信機(27)に供給される。この受信機(27)からは暗号化された情報信号S1*が出力され、デスクランブラ(28)に供給される。このデスクランブラ(28)では、例えばROM等の記憶装置

（29）より供給されるキー情報ＫＩに基づき、上述したスクランブラ（22）と逆の復号化処理がなされる。したがって、デスクランブラ（28）より導出された端子（30）には元の情報信号ＳＩが出力される。

（発明が解決しようとする問題点）

ところで、このようなスクランブル通信システムにおいて、キー情報ＫＩを故意に改ざんし、デスクランブラ（28）の出力信号を見ることができれば、暗号化のアルゴリズムを解読する手がかりとなってしまう。

本発明は、斯る点に鑑み、暗号化のアルゴリズムの解読が困難となるようにするものである。

（問題点を解決するための手段）

本発明は上述問題点を解決するため、記憶装置(1)にキー情報領域の他にチェックビット領域が設けられ、復号時記憶装置(1)のキー情報及びチェックビットが選択的に繰り返し指定されて論理演算がなされ、この演算結果が所定値となるときのみ、キー情報により暗号化された情報信号の復号化が行なわれるようにしたものである。

（作用）

以上の構成においては、正当ではない改ざんされたキー情報が供給されても、キー情報として扱われない。即ち、この正当でないキー情報が供給されるとき演算結果は所定値とならず、この正当でないキー情報による暗号化された情報信号の復号化は行なわれない。

（実施例）

以下、第１図を参照しながら本発明の一実施例について説明しよう。本例はスクランブル通信システムにおけるデスクランブラに適用した例である。

同図において、(1)は記憶装置を構成するＲＯＭである。第２図ＡはＲＯＭ(1)の内容を示したものである。即ち、ＲＯＭ(1)にはキー情報、チェックビットが書き込まれている。

このＲＯＭ(1)には、デスクランブラ(2)の制御信号発生器(3)より、第２図Ｂに示すように順次アドレス信号ＡＤ０～ＡＤ３が供給され、ＲＯＭ(1)の内容がパラレルデータとして順次繰り返し読み出される。

ＲＯＭ(1)からのデータはそのＭ系列を解くためのイクスクルーシブオア回路（ＥＸ－ＯＲ回路）(4)に供給される。また、Ｍ系列符号発生器(5)からのＭ系列符号はＥＸ－ＯＲ回路(4)に供給され、このＥＸ－ＯＲ回路(4)において、ＲＯＭ(1)からのデータのＭ系列が解かれる。

ＥＸ－ＯＲ回路(4)からのＭ系列の解かれたデータは、たたみ込み用のＥＸ－ＯＲ回路(6)を介してラッチ回路を構成するＤフリップフロップ（Ｄ－ＦＦ）(7)に供給される。Ｄ－ＦＦ(7)には、ＲＯＭ(1)よりデータが繰り返し読み出される例えば第１～第４の周期において、制御信号発生器(3)より第２図Ｃ１～Ｃ４に示すゲート信号ＧＡ１～ＧＡ４の高レベルのタイミングでクロックが供給され、ＥＸ－ＯＲ回路(6)からのデータがラッチされる。また、Ｄ－ＦＦ(7)の出力はＥＸ－ＯＲ回路(6)に供給される。

Ｄ－ＦＦ(7)には、制御信号発生器(3)より、各周期の初期のタイミングで第２図Ｄに示すようにクリア信号$\overline{\text{ＣＬＲ}}$が供給されてリセットされる。したがって、第１～第４の各周期の終わりにＤ－ＦＦ(7)には、夫々ゲート信号ＧＡ１～ＧＡ４の高レベルのタイミングでＥＸ－ＯＲ回路(6)によってたたき込まれたデータがラッチされている。

また、Ｄ－ＦＦ(7)の出力は正当性判定回路(9)に供給される。この正当性判定回路(9)では、第１～第４の各周期の終りにＤ－ＦＦ(7)にラッチされているデータの正当性が判定される。即ち、各ゲート信号ＧＡ１～ＧＡ４の高レベルのタイミングでＥＸ－ＯＲ回路(6)によってたたき込まれるデータの正当性が判定される。

また、（10）はキー情報のラッチ回路であり、このラッチ回路（10）にはＥＸ－ＯＲ回路(4)からＭ系列の解かれたデータが供給される。このラッ

チ回路（10）は上述した正当性判定回路(9)によって制御される。即ち、正当性判定回路(9)によって第1～第4の各周期の終りにD－FF(7)にラッチされているデータが全て所定値となり、正当であると判定されるときのみラッチ回路（10）が動作するようになされる。

ラッチ回路（10）には、制御信号発生器(3)より、第2図E1～E4に示すラッチ信号LA1～LA4のタイミングでクロックが供給され、キー情報がラッチされる。ラッチ回路（10）でラッチされたキー情報K1はデスクランブラ本体（図示せず）に供給され、このキー情報K1に基づいて復号化処理がなされる。

以上の構成においては、ROM(1)からのデータであるキー情報が正当なものであるとき、D－FF(7)にラッチされるデータは所定値となり、正当性判定回路(9)によってラッチ回路（10）は動作状態とされ、このラッチ回路（10）にキー情報K1がラッチされる。そして、デスクランブラ本体に供給されて復号化処理がなされる。一方、ROM(1)からのデータであるキー情報が正当なものでないとき、D－FF(7)にラッチされるデータは所定値とならず、正当性判定回路(9)によってラッチ回路（10）は動作状態とされず、このラッチ回路（10）にキー情報はラッチされない。そのため、このときのキー情報はデスクランブラ本体には供給されず、キー情報として取扱われない。

したがって、本例によれば、キー情報が例えば改ざんされて正当なものでなくなった場合には、このキー情報はデスクランブラ本体には供給されず、キー情報としては取扱われないので、キー情報等の改ざんによる暗号化のアルゴリズムの解読は困難となる。また、本例によれば第1～第4の周期の終りにD－FF(7)にラッチされているデータが全て所定値となるとき正当であると判定されるので、高精度の判定がなされる利益がある。

尚、上述実施例は、本発明をスクランブル通信システムにおけるデスクランブラに適用した例であるが、本発明は、記憶装置からのキー情報により暗号化された情報信号を復号化するその他の復号化装置にも同様に適用することができる。

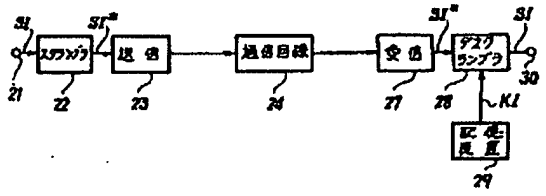
〔発明の効果〕

以上述べた本発明によれば、記憶装置からのキー情報が正当なものでない限りキー情報として取扱われないようにしたので、キー情報の改ざん等による暗号化のアルゴリズムの解読を良好に防止することができる。また、キー情報の正当性の判定はキー情報及びチェックビットが選択的に繰り返し指定されて行なわれるので、高精度の判定が可能となる利益がある。

図面の簡単な説明

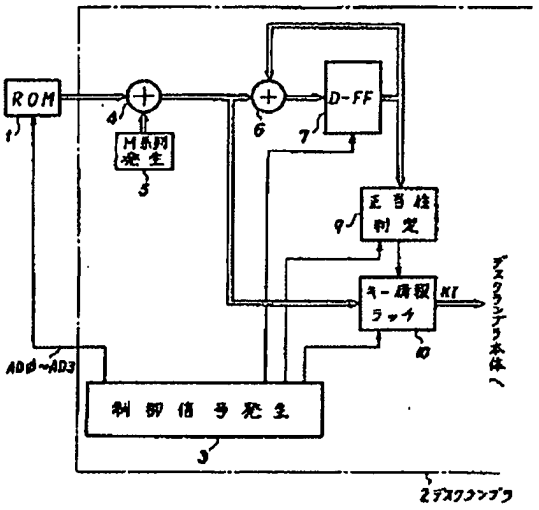
第1図は本発明の一実施例を示す構成図、第2図はその説明のための図、第3図はスクランブル通信システムの一例を示す図である。

(1)はROM、(2)はデスクランブラ、(3)は制御信号発生器、(4)及び(5)はイクスクルーシブオア回路、(7)はDフリップフロップ、(9)は正当性判定回路、（10）はキー情報ラッチ回路である。

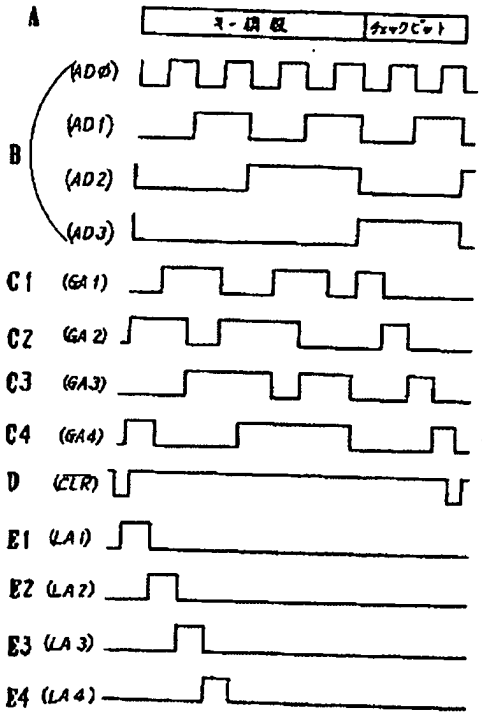


スクランブル通信システムの一例を示す図

第3図



実施例の構成図
第 1 図



第1図例の動作説明のための図
第 2 図